

EMN:SPN/PB
F. #2014R01719

15M229

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----- X

UNITED STATES OF AMERICA

- against -

YEHUDA KATZ,
also known as "Yehuda-Ari Katz,"

Defendant.

TO BE FILED UNDER SEAL

COMPLAINT AND AFFIDAVIT
IN SUPPORT OF APPLICATION
FOR ARREST WARRANT

(T. 18, U.S.C., § 1030(a)(4))

----- X
EASTERN DISTRICT OF NEW YORK, SS:

SAMAD D. SHAHRANI, being duly sworn, deposes and states that he is a Special Agent with the Federal Bureau of Investigation ("FBI"), duly appointed according to law and acting as such.

In or about and between May 2014 and August 2014, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant YEHUDA KATZ, also known as "Yehuda-Ari Katz," did knowingly and with intent to defraud, access a protected computer without authorization and exceed authorized access, and by means of such conduct furthered the intended fraud and obtained something of value, to wit: personal identifying information.

(Title 18, United States Code, Section 1030(a)(4)).

The source of your deponent's information and the grounds for his belief are as follows:¹

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). I have been employed by the FBI since 2011. My duties include the investigation and prosecution of violations pertaining to criminal computer intrusions. As a Special Agent with the FBI, I have participated in numerous investigations of criminal computer intrusions, during the course of which I have conducted or participated in surveillance, execution of search warrants, debriefings of informants, and reviews of documents and taped conversations. I have received specific training in matters relating to criminal computer investigations. On the basis of this familiarity, and on the basis of other information that I have reviewed and determined to be reliable, I submit the following information.

2. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from: (a) my personal participation in this investigation, (b) reports made to me by other law enforcement authorities, (c) information obtained from interviews with witnesses, and (d) review of other records and reports. The statements contained in this affidavit are based on my own observations and review of documents, or reliable information provided to me by other law enforcement personnel.

¹ Because the purpose of this Complaint is to set forth only those facts necessary to establish probable cause to arrest, I have not described all the relevant facts and circumstances of which I am aware.

I. THE INVESTIGATION

3. Since approximately August 2014, the FBI and the New York City Police Department, Internal Affairs Bureau (“NYPD-IAB”) have been conducting an ongoing criminal investigation into YEHUDA KATZ, also known as Yehuda-Ari Katz.

4. The government’s investigation has uncovered evidence that KATZ, an Auxiliary Deputy Inspector with the New York City Police Department (“NYPD”)’s 70th Precinct in Brooklyn, New York, surreptitiously installed multiple electronic devices in the Traffic Safety office of the 70th Precinct that allowed him to, among other things, remotely access certain restricted computers and sensitive law enforcement databases that he did not have permission to access. Further, it appears from the evidence that KATZ has attempted to fraudulently use information obtained from those law enforcement databases for his own financial gain.

5. On or about August 27, 2014, NYPD-IAB was contacted by officers assigned to the NYPD’s 70th Precinct. The officers reported that they had discovered a hidden camera in the 70th Precinct’s Traffic Safety office, a clerical office that maintains statistics and reports pertaining to car accidents and vehicular summonses.

6. On the same day, NYPD-IAB officers responded to the 70th Precinct and conducted a search of the Traffic Safety office. During their search, NYPD-IAB officers located the following two suspicious electronic devices:

a. The first device (“Device # 1”) included a small camera that was connected to a cable modem housed in a cable television box. The cable modem was connected, via a splitting device, to an existing cable line in the Traffic Safety office. Also included within the cable television box and connected to the modem was a wireless router.

b. The second device (“Device # 2”) was connected to one of the computers in the Traffic Safety office. Device # 2 was housed in a plastic box. The main component of Device # 2 is a Keyboard, Video and Mouse (“KVM”) device. When connected to a computer, a KVM device allows the computer to be accessed and controlled from a remote location. Using the KVM device, a remote user can control the computer’s keyboard and mouse and can view information displayed on the computer’s screen. The KVM device in Device # 2 was attached to a wireless receiver that would enable the KVM device to be operated without a wired Internet connection. Device # 2 also included a wireless Secure Digital (“SD”) memory card, which could be used for saving electronic files. In addition, Device # 2 included a Belkin International, Inc. (“Belkin”) WeMo switch, which allowed components of Device # 2 to be remotely switched on and off.

7. Subsequent forensic analysis of Device # 1 by law enforcement revealed that, before its discovery, Device # 1 was capable of capturing a live image of the Traffic Safety office and broadcasting that image to the Internet.

8. In addition, the forensic analysis of Device # 1 revealed the media access control (“MAC”) address of the cable modem housed inside Device # 1. A MAC address is a unique identifying number associated with digital devices that are capable of connecting to the Internet or some other network. Utilizing the MAC address for the modem, law enforcement obtained from Optimum Online – the Internet service provider (“ISP”) for the cable Internet connection in the 70th Precinct’s Traffic Safety office – the Internet protocol (“IP”) addresses² associated with the cable modem in Device # 1. This

² An IP address is a numerical label assigned to each device participating in a computer network.

information revealed that the modem in Device # 1 was first assigned an IP address on or about May 2, 2014.

9. NYPD-IAB also performed a forensic analysis of the computer that Device # 2 was connected to. NYPD-IAB confirmed that this computer was connected to the NYPD's network and to the Internet, and access to this computer was restricted to NYPD uniformed officers and certain civilian support staff. Notably, NYPD auxiliary officers were not permitted to access the computer. In order to gain access to the computer, a user would have to enter a unique username and a password. Based on its forensic analysis, NYPD-IAB was able to determine the usernames and passwords that had been used to log onto and access the computer that Device # 2 was connected to. Specifically, NYPD-IAB determined that between May 2, 2014, the day that the modem in Device # 1 was activated, and August 26, 2014, the day before Device # 1 and Device # 2 were discovered, the usernames and passwords for 15 NYPD officers were used to log onto the computer in question.

10. NYPD-IAB identified suspicious activity associated with the login information for three different NYPD officers. The activity associated with these three officers was suspicious because of (a) the timing of the logins and (b) what was done on the computer while the person or persons using the officers' logins were logged on. With respect to timing, the majority of the logins for the three officers in question occurred during times when the officers were either on their day off or on vacation. With respect to the activity that occurred during the logins, NYPD-IAB determined that, while the three officers' logins were in use, an abnormally high number of queries were run in the NYPD's accident index and "Z-Finest" databases. Specifically, between approximately May 2, 2014 and August 26, 2014, approximately 6,440 queries of license plates that had been involved in

traffic accidents in New York City were run in the Z-Finest system on the computer connected to Device # 2, all during times when one of the three officers' logins had been used to access the computer.³

11. Access to both the NYPD accident index and the Z-Finest database are restricted to NYPD uniformed officers and certain civilian support staff. Notably, NYPD auxiliary officers were not permitted to access these databases. NYPD personnel who are authorized to access these systems are required to enter a unique username and password in order to log on to the systems.⁴ In addition, both the NYPD accident index and the Z-Finest database can only be accessed via computers connected to the NYPD's computer network – in other words, the systems cannot be accessed remotely.

12. The NYPD accident index database maintains information about civilian car accidents, including but not limited to information regarding the license plates and drivers involved in the accidents. The Z-Finest database allows a user to query both New York and out-of-state vehicle license plates, vehicle identification numbers, and driver's licenses. The Z-Finest database is networked with and connected to the FBI's National Crime Information Center ("NCIC") database, which is maintained by the FBI's Criminal Justice Information Services Division in Clarksburg, West Virginia. As such, when a query is run in the Z-Finest system, it is also automatically run through the FBI's NCIC system.

13. In addition, forensic analysis was conducted on the SD memory card from Device # 2, which revealed that certain information – including accident and license

³ Following the August 27, 2014, discovery of Device # 1 and Device # 2, the number of Z-Finest queries run using three officers' login credentials decreased dramatically.

⁴ This is in addition to the username and password needed to log onto the computer itself.

plate reports – obtained from queries of the Z-Finest system and the NYPD accident index database was saved on the SD card. Law enforcement agents contacted several of the individuals whose license plates had been queried under the compromised passwords and whose information was found on the SD card.

14. For example, information about a May 22, 2014 traffic accident involving an individual with the initials K.G. was obtained after the investigation determined that K.G.'s license plate had been queried in the Z-Finest system from the computer connected to Device # 2. Specifically, NYPD-IAB determined that, on or about June 1, 2014, the license plate of K.G.'s car was queried in the Z-Finest system from the computer connected to Device # 2. On or about October 17, 2014, law enforcement agents spoke with K.G. During this conversation, K.G. confirmed that he/she had been in a traffic accident. K.G. further stated that, approximately two weeks after the accident, K.G. received a letter regarding the accident from someone purporting to be an attorney.

15. K.G. provided law enforcement with a copy of the letter that he/she had received after the traffic accident. The letter was dated June 2, 2014, and purported to be from an individual named "Yehuda-Ari Katz." The author of the letter stated that he was a "legal counselor" at "Katz and Katz law firm," and he signed the letter with a digital signature as "Y.A. Katz, Esq." The letter listed four purported offices of the "Katz and Katz" firm, as well as the names of 16 individuals who appeared to be lawyers with the firm. The letter included the following statements, among others:

a. "I can advise you with 100% confidence that I can resolve this claim in your favor."

b. “If I wasn’t sure for 100% that I can win your case I wouldn’t bother writing you this letter.”

c. “My past performance guarantees future results.”

d. “My fee is 14% only when you collect. And I know you will collect.”

16. NYPD-IAB determined that YEHUDA KATZ is an Auxiliary Deputy Inspector assigned to the NYPD’s 70th Precinct.⁵ As a NYPD Auxiliary officer, KATZ does not have permission to access the NYPD accident index or Z-Finest databases and he was never issued passwords for these databases.

17. According to a search of the attorney directory on the website of the New York State Unified Court System, YEHUDA KATZ does not appear as a licensed attorney in the State of New York. Further, while law enforcement agents located a law firm named “Katz & Katz, P.C.” based in New York, KATZ is not listed on that firm’s website as an attorney. In addition, the addresses listed on the letter sent to K.G. either do not exist or appear to correspond to unrelated businesses. Finally, while the individuals other than KATZ listed on the letter appear to be attorneys, they do not appear to work for the “Katz & Katz, P.C.” law firm. In fact, with the exception of KATZ, all of the individuals listed currently practice or formerly practiced at a large international law firm.

18. The letter from YEHUDA KATZ to K.G. listed a contact phone number of 646-399-2100. Information obtained from MetroPCS revealed that this phone

⁵ NYPD Auxiliary officers are volunteers who are trained and equipped by the NYPD, and they assist with certain non-enforcement or non-hazardous duties. However, they are not uniformed police officers.

number was active between approximately April 25, 2014 and July 14, 2014 and was subscribed to an individual named “Yehvdoi Katz.” Toll records for 646-399-2100 reveal multiple calls made from that number to the NYPD’s 70th Precinct auxiliary office. Toll records also reveal incoming telephone calls from approximately 65 phone numbers associated with individuals who had records of traffic accidents and a subsequent Z-Finest inquiry from the 70th Precinct. In addition, approximately 10 telephone numbers with incoming or outgoing calls to/from 646-399-2100 are associated with medical clinics, law firms, or chiropractors.

19. The letter sent to K.G. also listed a contact email address of “LegalReferralsNY@gmail.com”. Information obtained from Google, Inc. revealed that the “LegalReferralsNY@gmail.com” email address was registered to YEHUDA KATZ. In addition, Google provided a list of the IP addresses used to access the “LegalReferralsNY@gmail.com” email address. Among other things, this information revealed that, on at least one occasion, the IP address used to access the “LegalReferralsNY@gmail.com” email address was assigned to the cable modem Internet connection associated with Device # 1 – meaning that the person accessing the “LegalReferralsNY@gmail.com” email address was using the Internet connection associated with Device # 1.

20. On December 18, 2014, the Honorable Roanne L. Mann, United States Magistrate Judge for the Eastern District of New York, signed a search warrant for the “LegalReferralsNY@gmail.com” email address.

21. In response to the above-referenced search warrant, Google, Inc. provided various emails sent to and from the “LegalReferralsNY@gmail.com” email

address. Among other things, the emails showed that YEHUDA KATZ appeared to be the user of the “LegalReferralsNY@gmail.com” email account. In addition, law enforcement agents found emails where KATZ appeared to be negotiating to purchase a cable television box of the same make and model as the cable television box used in Device # 1. Law enforcement agents also located numerous emails between KATZ and other individuals that referenced automobile accidents.

22. On or about November 26, 2014, one of the law enforcement agents working on this investigation spoke with an investigator with the National Insurance Crime Bureau (“NICB”)’s Major Medical Fraud Task Force.⁶ That investigator relayed that, in the course of one of his investigations, he had identified a letter that was very similar to the letter referenced above from “Yehuda-Ari Katz.” The investigator provided law enforcement agents working on this investigation with a copy of the letter.

23. The letter in question purports to be from an individual named “Jeffrey Goodwin.” In style and in substance, it appears very similar to the letter referenced above from “Yehuda-Ari Katz.” For example:

a. As was the case in the letter from “Yehuda-Ari Katz,” the author of the “Jeffrey Goodwin” letter refers to himself as a “legal counselor.”

b. As was the case in the letter from “Yehuda-Ari Katz,” the author of the “Jeffrey Goodwin” letter signed the letter with a digital signature and in a font that appears to be the same as the font used in the “Yehuda-Ari Katz” letter.

⁶ According to their website, the NICB is a non-profit organization created by the insurance industry to address insurance-related crimes. The NICB works closely with law enforcement agencies.

c. As was the case in the letter from “Yehuda-Ari Katz,” the author of the “Jeffrey Goodwin” letter stated: “I can advise you with 100% confidence that I can resolve this claim in your favor.”

d. As was the case in the letter from “Yehuda-Ari Katz,” the author of the “Jeffrey Goodwin” letter stated: “If I wasn’t 100% sure that I can win your case I wouldn’t bother writing you this letter.”⁷

e. As was the case in the letter from “Yehuda-Ari Katz,” the author of the “Jeffrey Goodwin” letter stated: “My past performance guarantees future results.”

f. Attached to both the “Yehuda-Ari Katz” and “Jeffrey Goodwin” letters is a second page entitled “Frequently Asked Questions.” The questions and answers listed are substantially the same for both letters.

24. The letter sent by “Jeffrey Goodwin” also listed a contact email address of “jeffdoodlaw@gmail.com”. Information obtained from Google pursuant to a grand jury subpoena revealed that the “jeffdoodlaw@gmail.com” email address did not exist. Based on the fact that author of the letter claimed to be named “Goodwin,” law enforcement agents subpoenaed Google for information related to the email address “jeffgoodlaw@gmail.com.” Information obtained from Google revealed that the “jeffgoodlaw@gmail.com” email address was registered to “Jeff Goodwin.” The email account was created on July 14, 2014. In addition, Google provided a list of the IP addresses used to access the “jeffgoodlaw@gmail.com” email address. Among other things, this information revealed

⁷ In the letter from “Yehuda-Ari Katz,” there appeared to be a typographical error that was fixed in the “Jeffrey Goodwin” letter.

that, on multiple occasions, the IP address used to access the “jeffgoodlaw@gmail.com” email address was assigned to the cable modem Internet connection associated with Device # 1 – meaning that the person accessing the “jeffgoodlaw@gmail.com” email address was using the Internet connection associated with Device # 1.

25. Based on conversations with the NICB investigator, law enforcement agents were able to determine the name of the individual to whom the “Jeff Goodwin” letter was sent. In addition, it was determined that this individual, who has the initials W.S., had been involved in a traffic accident in New York City on or about August 14, 2014. Law enforcement agents working on this investigation were also able to determine that, on or about August 16, 2014, W.S.’s license plate number was queried in the Z-Finest system on the computer that connected to Device # 2.

26. In addition, emails obtained from the search warrant returns for the “LegalReferralsNY@gmail.com” email address revealed that, on approximately July 2, 2014, YEHUDA KATZ registered for a service called TrapCall. Based on a review of TrapCall’s publicly-available website, TrapCall purports to be a caller ID unblocking service – that is, a service that unmask blocked or private numbers on the subscriber’s cell phone. TrapCall is downloaded as an application on a smartphone. TrapCall also purports to provide voicemail functionality. The subscriber’s voicemails are not stored on the cell phone, but instead are saved online and the subscriber can access the emails via the internet.

27. Information obtained via grand jury subpoena to TrapCall revealed, among other things, that YEHUDA KATZ signed up for an account on July 2, 2014. The name of the subscriber on the account was “Yehuda Katz.” The initial email address associated with the TrapCall account was “LegalReferralsNY@gmail.com”, however, the

email address associated with the TrapCall account was changed to the “jeffgoodlaw@gmail.com” email address. In addition, the initial phone number on the account was 646-399-2100, the phone number on the “Yehuda-Ari Katz” letter, but the phone number was changed to 212-470-1772, which is the phone number on the “Jeffrey Goodwin” letter.

28. In January 2015, Belkin provided information about the WeMo switch in Device # 2 in response to a subpoena. The information provided by Belkin revealed, among other things, that the WeMo switch was activated on June 17, 2014. It was further revealed that only one device, a Samsung SGH-T599N with the “Device ID” of 356433051301896, was used to control the WeMo switch in Device # 2. Notably, based on information obtained from MetroPCS, the mobile phone registered to “Yehvdoi Katz” and which law enforcement agents believe is used by YEHUDA KATZ is a Samsung SGH-T599N with the ESN/MEID⁸ of 356433051301896. Finally, the information obtained from Belkin revealed that the device used to control the WeMo switch in Device # 2 was assigned IP addresses registered to T-Mobile USA and Optimum Online. Notably, MetroPCS, the cell phone provider for the “Yehvdoi Katz” cell phone, is owned by T-Mobile USA, and the Internet provider for the Traffic Safety Office for the NYPD’s 70th Precinct is Optimum Online. Based on this information, as well as my training and experience, I believe that it was KATZ who was controlling the Belkin WeMo switch in Device # 2.

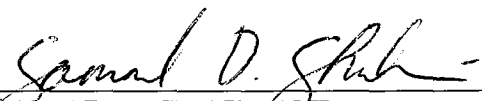
⁸ An ESN/MEID is a globally unique identifying number identifying a physical piece of mobile equipment.

II. CONCLUSION

29. Based on the facts set forth in this affidavit, there is probable cause to believe that the defendant YEHUDA KATZ, also known as “Yehuda-Ari Katz,” did knowingly and with intent to defraud, access a protected computer without authorization and exceed authorized access, and by means of such conduct furthered the intended fraud and obtained something of value, to wit: personal identifying information, in violation of Title 18, United States Code, Section 1030(a)(4).


30. It is respectfully requested that this Court issue and order sealing, until further order of the Court, all papers submitted in support of this application, including the application, the arrest warrant, and the complaint. I believe that sealing these documents is necessary because the defendant is currently at liberty. Thus, the government seeks to seal the complaint and arrest warrant to ensure that the defendant does not learn that a complaint has been filed and an arrest warrant has been issued, and to prevent him from fleeing justice and avoiding arrest and prosecution.

WHEREFORE, your deponent respectfully requests that an arrest warrant be issued, and that the defendant YEHUDA KATZ be dealt with according to law.



SAMAD D. SHAHRANI
Special Agent
Federal Bureau of Investigation

Sworn to me before this
12th day of March 2015



THE HONORABLE LOIS BLOOM
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK